

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-258910

(43)Date of publication of application : 12.09.2003

(51)Int.Cl.

H04L 12/56

G06F 13/00

G06F 15/00

H04L 12/22

(21)Application number : 2002-056913

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 04.03.2002

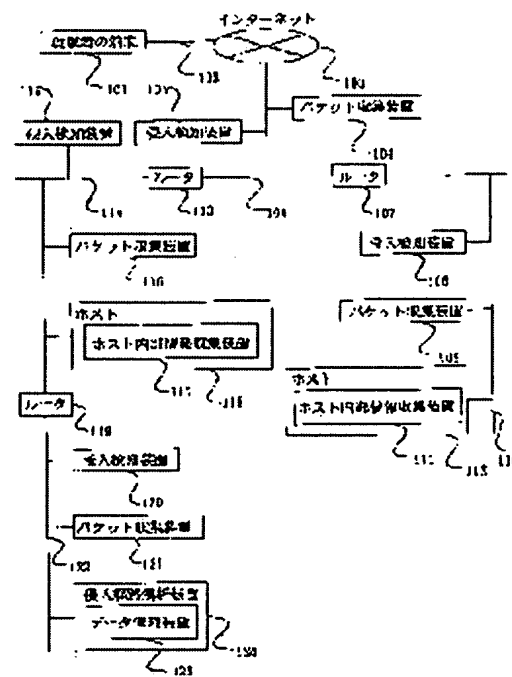
(72)Inventor : KITAZAWA SHIGEKI

## (54) SYSTEM AND METHOD FOR ANALYZING ILLEGAL ACCESS ROUTE

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To realize intrusion route analysis which is applicable to intrusion using a steppingstone and intrusion using a false transmission-source address.

**SOLUTION:** A packet gathering device 104, etc., records the header contents of a packet sent through a network as header information and a host internal information gathering device 111, etc., gathers internal process information regarding internal processes of a host 112, etc. An intrusion route analyzing device 124 receives the header information and internal process information and a data management device 123 manages data as a database; when an intrusion packet is detected, the transmission source of the intrusion packet is detected by using host level analysis and router level analysis in combination and when the transmission source of the intrusion packet is a host in the network, a packet which contributes the generation and transmission of the intrusion packet is specified by taking host internal analysis of the host to analyze the intrusion route by using the three analyzing processes in combination.



## LEGAL STATUS

[Date of request for examination]

25.02.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than

the examiner's decision of rejection or  
application converted registration]

[Date of final disposal for application]

[Patent number] 3892322

[Date of registration] 15.12.2006

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2003-258910  
(P2003-258910A)

(43) 公開日 平成15年9月12日 (2003.9.12)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
H 0 4 L 12/56	4 0 0	H 0 4 L 12/56	4 0 0 Z 5 B 0 8 5
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 9
15/00	3 2 0	15/00	3 2 0 A 5 K 0 3 0
H 0 4 L 12/22		H 0 4 L 12/22	

審査請求 未請求 請求項の数16 O L (全 16 頁)

(21) 出願番号 特願2002-56913 (P2002-56913)

(22) 出願日 平成14年3月4日 (2002.3.4)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 北澤 繁樹

東京都千代田区丸の内二丁目2番3号 三  
菱電機株式会社内

(74) 代理人 100099461

弁理士 溝井 章司 (外5名)

Fターム(参考) 5B085 AC11

5B089 GB02 KA17 KB13

5K030 GA15 HA08 JA10 KA05 KX24

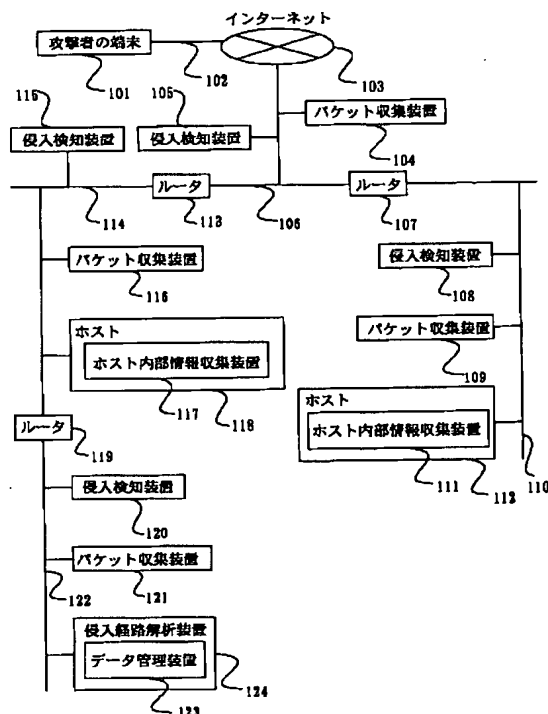
KX30 LC14 LC15 LD19

(54) 【発明の名称】 不正アクセス経路解析システム及び不正アクセス経路解析方法

(57) 【要約】

【課題】 踏み台を用いた侵入、発信元アドレスを詐称した侵入に対しても対応可能な侵入経路解析を実現する。

【解決手段】 パケット収集装置104等がネットワーク上を流れるパケットのヘッダ内容をヘッダ情報として記録し、ホスト内部情報収集装置111等がホスト112等の内部プロセスに関する内部プロセス情報を収集し、侵入経路解析装置124はヘッダ情報及び内部プロセス情報を受信するとともにデータ管理装置123においてデータベースとして管理し、侵入パケットの検知の際に、ホストレベル解析及びルータレベル解析を併用して侵入パケットの送信元を検出し、侵入パケットの送信元がネットワーク内のホストであった場合には、当該ホストに対してホスト内部解析を行って侵入パケットの生成・送信に関与したパケットを特定し、以後、3つの解析処理を併用して侵入経路の解析を行う。



## 【特許請求の範囲】

【請求項 1】 相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、

前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、

前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析システム。

【請求項 2】 前記不正アクセス経路解析システムは、更に、

前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行う内部プロセス監視部を有し、

前記内部プロセス解析処理部は、

前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする請求項 1 に記載の不正アクセス経路解析システム。

【請求項 3】 前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行

い、

前記送信元検出処理部は、

前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行い、所定の場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、

前記内部プロセス解析処理部は、

前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行うことを特徴とする請求項 1 又は 2 に記載の不正アクセス経路解析システム。

【請求項 4】 前記内部プロセス解析処理部は、

特定のデータ処理装置の内部プロセスについて解析処理を行った結果、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする請求項 1～3 のいずれかに記載の不正アクセス経路解析システム。

【請求項 5】 前記不正アクセス経路解析システムは、データ処理装置間に少なくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、前記送信元検出処理部は、

不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次遡って不正アクセスパケットの送信元を検出する第一の送信元検出処理と、

不正アクセスパケットに含まれた送信元を示す送信元アドレス情報に基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行うことを特徴とする請求項 1～3 のいずれかに記載の不正アクセス経路解析システム。

【請求項 6】 前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があります、

前記内部プロセス解析処理部は、

前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、

前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセス

についての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする請求項5に記載の不正アクセス経路解析システム。

【請求項7】 前記不正アクセス経路解析システムは、更に、  
前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流通する複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報として記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット収集部を有し、  
前記送信元検出処理部は、  
前記パケット収集部より前記複数のヘッダ情報を受信するとともに、  
前記第一の送信元検出処理として、  
データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元E t h e r アドレス、宛先E t h e r アドレス及びT T L ( T i m e T o L i v e ) 値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元E t h e r アドレス、宛先E t h e r アドレス及びT T L 値を始点として抽出ヘッダ情報に含まれる送信元E t h e r アドレス、宛先E t h e r アドレス及びT T L 値の更新経過を順次遡って不正アクセスパケットの送信元を検出することを特徴とする請求項5に記載の不正アクセス経路解析システム。  
【請求項8】 前記送信元検出処理部は、  
前記第二の送信元検出処理として、  
不正アクセスパケットに含まれた送信元I P アドレスに基づき、不正アクセスパケットの送信元を検出することを特徴とする請求項5に記載の不正アクセス経路解析システム。  
【請求項9】 前記パケット収集部は、  
前記送信元検出処理部から指示があった場合のみ、パケットの収集を行うことを特徴とする請求項7に記載の不正アクセス経路解析システム。  
【請求項10】 前記パケット収集部は、  
前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする請求項7に記載の不正アクセス経路解析システム。  
【請求項11】 前記不正アクセス経路解析システムは、更に、  
前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報収集部を有し、  
前記内部プロセス解析処理部は、  
前記内部プロセス情報収集部より前記内部プロセス情報

を受信するとともに、受信した内部プロセス情報の中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする請求項1～3のいずれかに記載の不正アクセス経路解析システム。

【請求項12】 前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の収集を行うことを特徴とする請求項11に記載の不正アクセス経路解析システム。

【請求項13】 前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする請求項11に記載の不正アクセス経路解析システム。

【請求項14】 前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、前記送信元検出処理部は、

前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行うことを特徴とする請求項1に記載の不正アクセス経路解析システム。

【請求項15】 前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、

前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする請求項1に記載の不正アクセス経路解析システム。

【請求項16】 相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析方法であって、

前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、  
前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理ステップと、  
前記送信元検出処理ステップにより特定のデータ処理装

置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、前記送信元検出処理ステップは、前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする不正アクセス経路解析方法。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】この発明は、侵入経路解析システム並びに、侵入経路解析手法の高速化に関するものである。

##### 【0002】

【従来の技術】図2は例えば、特開2000-341315および特開2000-124952に示されたパケットの情報を解析する従来の侵入経路解析システムを示す。図2において、201は攻撃者端末、202はインターネット、203は攻撃者端末が直接接続しているアクセスサーバ、206は踏み台ホスト、211は不正アクセス対象ホスト、210は侵入検知装置、204、205は攻撃者端末201から踏み台ホスト206へのパケットを中継した追跡装置（ルータ）、207、208、209は踏み台ホストから不正アクセス対象ホストへのパケットを中継した追跡装置（ルータ）である。攻撃者は、踏み台ホスト206を使用することで不正アクセス対象ホスト211に対して攻撃者端末の身元を隠蔽して不正アクセスを行っているものとする。

【0003】このような従来の侵入追跡システムにおいては、不正アクセス対象ホスト211から踏み台ホスト206までの追跡と踏み台ホスト206から攻撃者端末201までの追跡処理が複数の段階を経る。どの段階においても不正アクセスパケットの情報を元に追跡管理装置212が追跡経路上に存在する複数の追跡装置（ルータ）へ追跡を指示し、その結果からさらにその先の追跡装置（ルータ）へ追跡を指示するといった逐次的な追跡を継続することで攻撃者端末201が直接接続しているアクセスサーバ203まで追跡を行う。最終的な攻撃者端末201の特定はアクセスサーバ203の接続ログを解析することで行う。

【0004】図3は例えば、特開平10-164064に示された接続経路情報をホスト間の接続ごと、あらかじめ記録として残しておく従来の侵入経路解析システム

である。図3において、301はネットワーク管理マネージャ、302、303、304は計算機ノード、305は追跡情報収集操作、306はセキュリティ上の問題通知を表している。図において、計算機ノード302から計算機ノード303を踏み台として、計算機ノード304へ不正なアクセスを行っているものとする。また、各計算機ノードは、リモートから接続が行われたとき、その接続の経路追跡を行うための情報をあらかじめ記録しておく。

【0005】このような従来の侵入追跡システムにおいては、図3の計算機ノード303から計算機ノード304へ接続を要求した場合、計算機ノード304は、経路追跡に使用する接続経路情報を計算機ノード303へ要求する。計算機ノード303は、接続を要求している計算機ノード303上のプロセスの識別子と計算機ノード303の識別子を計算機ノード304へ送る。同様の手続きは、計算機ノード間の接続が発生するたびに行われているものとする。セキュリティ上の問題が計算機ノード304上で起こったとき、ネットワーク管理マネージャ301は計算機ノード304からのセキュリティ上の問題通知306を受け取り、計算機ノード304上に記録されている、そのセキュリティ上の問題を発生させる元となった接続経路情報を元に、計算機ノード303へ計算機ノード304との接続経路情報を問い合わせる。計算機ノード303では、計算機ノード304への接続は計算機ノード302からの接続により起動されたプロセスにより発生していることをネットワーク管理マネージャ301へ通知する。次にネットワーク管理マネージャ301は、計算機ノード302へ接続経路情報の問い合わせを行い、最終的に計算機ノード302が不正なアクセスを行った接続経路の発信源であると特定する。

##### 【0006】

【発明が解決しようとする課題】従来の侵入経路解析システムのうち、特開2000-341315及び特開2000-124952に示されたものは、パケットのヘッダ情報を元に侵入経路を解析することでIPパケットのヘッダ情報に含まれている発信元アドレスを詐称した不正アクセスパケットの追跡が可能という利点がある反面、踏み台を介した攻撃については、踏み台ホストの入出力を監視し、不正アクセスパケットが再び踏み台ホストへ送信されるのを待つ必要があり、侵入経路追跡の継続性を積極的に維持できない、追跡時間がかかるなどの問題点があった。一方、接続経路情報をホスト間の接続ごとにあらかじめ記録として残しておく方式（特開平10-164064）では、侵入経路追跡にかかる時間を短縮できる代わりに、IPパケットのヘッダ情報に含まれている発信元アドレスを詐称した攻撃では、偽の接続経路情報が記録されることもありうるため、正確性に問題点があった。また、いずれの場合にも追跡処理を管理するホストが侵入経路上のルータもしくは、接続ホスト

一つ一つと通信を行いながら逐次追跡していくため、侵入経路上のルータおよびホストの数に比例して侵入経路解析時間が増加する問題点があった。

【0007】この発明は上記のような問題点を解決するためになされたもので、攻撃者が身元を隠蔽する行為

(例えば発信元IPアドレスの詐称、踏み台ホストの使用など)を行った場合であっても侵入経路解析結果を正確かつ高速に求めることができる侵入経路解析システムのためのシステム構成と解析アルゴリズムに関するものである。

【0008】

【課題を解決するための手段】本発明に係る不正アクセス経路解析システムは、相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析システムであって、前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視部と、前記パケット監視部により不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理部と、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理部とを有し、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0009】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々の内部プロセスを監視し、所定の場合に、前記内部プロセス解析処理部に特定のデータ処理装置に関する通知を行う内部プロセス監視部を有し、前記内部プロセス解析処理部は、前記内部プロセス監視部から通知されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われた場合

に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0010】前記送信元検出処理部及び前記内部プロセス解析処理部は、相互に連動してそれぞれの処理を行い、前記送信元検出処理部は、前記内部プロセス解析処理部により不正アクセスパケットの認定が行われる度に、認定された不正アクセスパケットの送信元の検出処理を行い、所定の場合に、特定のデータ処理装置を不正アクセスパケットの送信元として検出し、前記内部プロセス解析処理部は、前記送信元検出処理部により特定のデータ処理装置が不正アクセスパケットの送信元として検出される度に、前記送信元検出処理部により検出されたデータ処理装置の内部プロセスについて解析処理を行い、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出された場合に、不正アクセスパケットの認定を行うことを特徴とする。

【0011】前記内部プロセス解析処理部は、特定のデータ処理装置の内部プロセスについて解析処理を行った結果、不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスが検出されなかった場合に、前記特定のデータ処理装置を不正アクセスの始点と判断することを特徴とする。

【0012】前記不正アクセス経路解析システムは、データ処理装置間に少なくとも一つ以上のパケット中継装置が配置されたネットワークを管理対象とし、前記送信元検出処理部は、不正アクセスパケットを受信したデータ処理装置を始点として、不正アクセスパケットを中継したパケット中継装置を論理的に順次遡って不正アクセスパケットの送信元を検出する第一の送信元検出処理と、不正アクセスパケットに含まれた送信元を示す送信元アドレス情報に基づき、不正アクセスパケットの送信元を検出する第二の送信元検出処理とを並行して行うことを特徴とする。

【0013】前記第二の送信元検出処理は前記第一の送信元検出処理よりも早期に完了する場合があります。前記内部プロセス解析処理部は、前記第二の送信元検出処理が前記第一の送信元検出処理よりも早期に完了し、不正アクセスパケットの送信元として特定のデータ処理装置が検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについて解析処理を行い、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理の実行中に、前記第一の送信元検出処理が完了し前記第二の送信元検出処理とは異なるデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記第二の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を終了し、前記第一の送信元検出処理により検出されたデータ処理装置の内部プロセスについての解析処理を開始することを特徴とする。

【0014】前記不正アクセス経路解析システムは、更に、前記ネットワーク内の少なくとも一以上の箇所で前記ネットワークを流通する複数のパケットを収集し、収集した複数のパケットのヘッダの内容を複数のヘッダ情報として記録し、記録した複数のヘッダ情報を前記送信元検出処理部に送信するパケット収集部を有し、前記送信元検出処理部は、前記パケット収集部より前記複数のヘッダ情報を受信するとともに、前記第一の送信元検出処理として、データ処理装置が受信した不正アクセスパケットのヘッダに含まれる情報であって送信元Ethernetアドレス、宛先Ethernetアドレス及びTTL(Time To Live)値以外の情報に基づき、前記複数のヘッダ情報の中から少なくとも一つ以上のヘッダ情報を抽出ヘッダ情報として抽出し、不正アクセスパケットに含まれる送信元Ethernetアドレス、宛先Ethernetアドレス及びTTL値を始点として抽出ヘッダ情報に含まれる送信元Ethernetアドレス、宛先Ethernetアドレス及びTTL値の更新経過を順次遡って不正アクセスパケットの送信元を検出することを特徴とする。

【0015】前記送信元検出処理部は、前記第二の送信元検出処理として、不正アクセスパケットに含まれた送信元IPアドレスに基づき、不正アクセスパケットの送信元を検出することを特徴とする。

【0016】前記パケット収集部は、前記送信元検出処理部から指示があった場合のみ、パケットの収集を行うことを特徴とする。

【0017】前記パケット収集部は、前記送信元検出処理部から指示があった場合のみ、前記送信元検出処理部に対して前記複数のヘッダ情報を送信することを特徴とする。

【0018】前記不正アクセス経路解析システムは、更に、前記複数のデータ処理装置の各々について内部プロセスに関する情報を内部プロセス情報として収集し、収集した内部プロセス情報を前記内部プロセス解析処理部へ送信する内部プロセス情報収集部を有し、前記内部プロセス解析処理部は、前記内部プロセス情報収集部より前記内部プロセス情報を受信するとともに、受信した内部プロセス情報の中から内部プロセス解析処理の対象となるデータ処理装置の内部プロセス情報を選択し、選択した内部プロセス情報を用いて内部プロセス解析処理を行うことを特徴とする。

【0019】前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、内部プロセス情報の収集を行うことを特徴とする。

【0020】前記内部プロセス情報収集部は、前記内部プロセス解析処理部から指示があった場合のみ、前記内部プロセス解析処理部に対して前記内部プロセス情報を送信することを特徴とする。

【0021】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路

解析システムと通信可能であり、前記他の不正アクセス経路解析システムより、前記他のネットワーク内で検出された他ネットワーク不正アクセスパケットの情報を含む検出依頼を受信した場合に、前記送信元検出処理部は、前記検出依頼に含まれた前記他ネットワーク不正アクセスパケットの情報に基づき、前記他ネットワーク不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0022】前記不正アクセス経路解析システムは、他のネットワークを管理対象とする他の不正アクセス経路解析システムと通信可能であり、前記送信元検出処理部が特定の不正アクセスパケットについて送信元が検出できなかった場合に、前記他の不正アクセス経路解析システムに対して前記特定の不正アクセスパケットの送信元の検出を依頼する検出依頼を送信することを特徴とする。

【0023】本発明に係る不正アクセス経路解析方法は、相互にパケット送受信を行い得る複数のデータ処理装置を含む所定のネットワークを管理対象とし、前記ネットワークに含まれるいずれかのデータ処理装置に対して不正アクセスパケットが送信された場合に、不正アクセスパケットの送信に用いられた不正アクセス経路の解析を行う不正アクセス経路解析方法であって、前記ネットワークを流通するパケットを監視し、不正アクセスパケットを検知するパケット監視ステップと、前記パケット監視ステップにより不正アクセスパケットが検知された場合に、不正アクセスパケットの送信元の検出処理を行い、所定の場合に、前記複数のデータ処理装置のうち特定のデータ処理装置を不正アクセスパケットの送信元として検出する送信元検出処理ステップと、前記送信元検出処理ステップにより特定のデータ処理装置が不正アクセスパケットの送信元として検出された場合に、前記送信元検出処理ステップにより検出されたデータ処理装置の内部プロセスについて解析処理を行って、不正アクセスパケットの生成及び送信を実行した内部プロセスを不正アクセスパケット生成送信プロセスとして検出するとともに、所定の場合に、前記不正アクセスパケット生成送信プロセスに関連するパケット受信プロセスを検出し、検出した前記パケット受信プロセスにおいて受信されたパケットを不正アクセスパケットとして認定する内部プロセス解析処理ステップとを有し、前記送信元検出処理ステップは、前記内部プロセス解析処理ステップにより不正アクセスパケットの認定が行われた場合に、認定された不正アクセスパケットの送信元の検出処理を行うことを特徴とする。

【0024】

【発明の実施の形態】実施の形態1. 図1は侵入経路解析システム(不正アクセス経路解析システム)の全体図を表す構成図である。ただし、図1はこの侵入経路解析システムの最小単位を示しており、図9のようにそれぞ



れが連携することにより、さらに大きなシステムを構成できる（実施の形態5）。図において、101は攻撃者の端末、102は攻撃者がインターネットへ接続している経路、103はインターネット、107、113、119はルータ、105、108、115、120は侵入検知装置、112、118はホスト、111、117はホスト内部情報収集装置、104、109、116、121はパケット収集装置、106、110、114、122はサブネットワーク、123はデータ管理装置、124は侵入経路解析装置である。ここで、サブネットワークはホスト（複数可）とその他の接続端末によって形成されるローカルネットワークを表す。サブネットワーク（複数可）は、ルータによって相互接続している。図1では、作図の便宜上、ルータ、ホストなどの総数を制限して図示しているが、実運用する場合の総数を制限するものではない。また、図の各装置の配置も実運用の形態を制限するものではないが、1サブネットワーク当たり、最低1つのパケット収集装置を配置する。さらに、ホストが存在するサブネットワークには、最低1つの侵入検知装置が存在し、各ホストにホスト内部情報収集装置が存在するものとする。図1に示す侵入検知装置105、108、115、120、ホスト内部情報収集装置111、117、パケット収集装置104、109、116、121、侵入経路解析装置124により構成されるシステムは、本発明に係る不正アクセス経路解析システムの一例に相当する。

【0025】図1において、侵入検知装置105、108、115、120は、それぞれに割当てられたサブネットワーク上を流れるパケットを監視し、所定の場合に、侵入パケット（不正アクセスパケット又は攻撃パケットともいう）を検知する。侵入検知装置は、パケット監視部に相当する。なお、図1には示していないが、ホスト112、118の内部プロセス実行状態を監視し、内部プロセスに異常があった場合に侵入があったと判断する侵入検知装置を設けてもよい。このような内部プロセスを監視して侵入を検知する侵入検知装置は、内部プロセス監視部に相当する。ホスト内部情報収集装置111、117は、それぞれが対象とするホストの内部プロセスに関するホスト内部情報を収集し、収集したホスト内部情報を侵入経路解析装置124へ送信する。ホスト内部情報収集装置は、内部プロセス情報収集部に相当する。パケット収集装置104、109、116、121は、それぞれが接続されているサブネットワーク上を流れるパケットを捕捉し、捕捉したパケットのヘッダの内容を記録する。記録したヘッダの内容をヘッダ情報と呼ぶ。パケット収集装置は、パケット収集部に相当する。侵入経路解析装置124は、パケット収集装置よりヘッダ情報を、ホスト内部情報収集装置よりホスト内部情報を、それぞれ受信し、ヘッダ情報に基づきルータレベル解析及びホストレベル解析を行い、ホスト内部情報に基

づきホスト内部解析を行う。侵入経路解析装置124は、送信元検出処理部と内部プロセス解析処理部に相当する。なお、ルータレベル解析、ホストレベル解析、ホスト内部解析の詳細については後述する。また、ホスト112、118は、データ処理装置に、ルータ107、113、119はパケット中継装置に相当する。

【0026】次に動作について説明する。まず、侵入経路解析装置124で侵入経路解析を行うための準備段階としてパケット収集装置並びに、ホスト内部情報収集装置による情報収集を行う。パケット収集装置104、109、116、121はそれぞれが接続されているサブネットワーク106、110、114、122を流れるパケットを捕捉し、ヘッダの内容をヘッダ情報として記憶領域に記録する。記録するパケットの情報は、パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の発信元Ethernetアドレス、宛先Ethernetアドレス、ICMPプロトコルヘッダのType、Code、Checksum、IPプロトコルヘッダのIdentification、TTL（Time To Live）、Protocol、発信元IPアドレス、宛先IPアドレス、TCP/UDPプロトコルヘッダの発信元ポート番号、宛先ポート番号、Checksum、TCPプロトコルヘッダのSequence Number、Acknowledgment Numberなどの情報を含む。ホスト内部情報収集装置はホスト上のプロセス管理情報として、プロセス生成日時、プロセス終了日時、プロセス識別子、親プロセス識別子、実ユーザ識別子、実行ユーザ識別子、実グループ識別子、実行グループ識別子、実行ディレクトリ、実行コマンドパス、実行コマンドライン、通信開始日時、通信終了日時、通信先IPアドレス、通信先TCP/UDPポート番号、通信NICに割り当てられていたEthernetアドレスとIPアドレス、TCP/UDPポート番号などの情報を収集する。収集、記録したこれらの情報は定期的にデータ管理装置123へ送信される。データ管理装置123は受信したデータを各項目ごとに関連付けてデータベースへ記録する。

【0027】侵入経路解析装置124は、各サブネットワーク上を流れるパケットを監視している侵入検知装置105、108、115、120からの侵入検知報告が発生した場合に、自動または手動によって侵入経路解析を開始する。ただし、侵入経路解析を開始する時点において、侵入検知時刻以前にパケット収集装置104、109、116、121並びに、ホスト内部情報収集装置111、117によって収集されたデータは、定期的にデータ管理装置123へ送信され、既にデータベースに格納済みであるものとする。

【0028】ここでは、図1並びに、図4を参照しながら、侵入経路解析装置124で行われる侵入経路解析スケジューリングについて説明する。図4は、侵入経路解

析スケジューリングをそれぞれの解析時系列(414、415、416)上に表したものである。図4において、解析時系列(414、415、416)上の長方形は、その解析が実行中であることを示している。図4において、414はホストレベル解析を、415はホスト内部解析を、416はルータレベル解析を示している。

【0029】ホストレベル解析は、侵入検知装置により検知された侵入パケットに含まれた送信元IPアドレスに基づき、侵入パケットの送信元を検出する解析手法である。また、パケットがたとえばRFC(Request for Comments)で規定されるような通信プロトコルに違反していないかどうかの解析も行う。また、パケットのヘッダ情報に含まれる発信元IPアドレスが実際にネットワークへ接続可能なIPアドレスであるかどうかなどの調査(DNSの参照やパケット到達性の検査)もあわせて行う。したがって、一般的には短時間で解析処理が終了する反面、IPアドレスを詐称された場合に対応できないため、解析結果の正確性に乏しい。なお、ホストレベル解析は、第二の送信元検出処理に相当する。一方、ルータレベル解析は、パケット収集装置より送信されたヘッダ情報のうち送信元Etherアドレス、宛先Etherアドレス、TTLに基づいて、侵入パケットを中継したルータを論理的に順次遡って侵入パケットの送信元を検出する解析手法である。ルータレベル解析は、パケットのIPアドレスによらず解析を行うので、IPアドレスを詐称された場合でも正確にパケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。なお、ルータレベル解析の具体的手順については後述する。また、ルータレベル解析は、第一の送信元検出処理に相当する。ホスト内部解析は、ホストレベル解析、ルータレベル解析によりホストが特定された場合、またはホスト内部を監視する侵入検知装置によりホストが特定された場合に、特定されたホストの内部プロセス状況を解析し、そのホストが侵入パケットの生成及び送信を行ったか否かを判断するとともに、そのホストが受信したパケットのうち侵入パケットの生成及び送信に関与したパケットを特定する解析手法である。ホスト内部解析の具体的手順についても後述する。

【0030】図1の侵入経路解析装置124は以下の解析の開始および終了の条件に従って侵入経路解析を継続もしくは終了する。ネットワークを流れるパケットを監視している侵入検知装置からの侵入検知通知があった場合には、まず、ホストレベル解析とルータレベル解析を平行して実行する(401、409)。また、ホストの内部状態を監視する侵入検知装置から侵入検知通知があった場合には、まず、ホスト内部解析を実行する。ホストレベル解析終了時(402、403、404)、そのホストレベル解析と同時に開始されたルータレベル解析(たとえば、401で開始されたホストレベル解析に対

する409で開始されたルータレベル解析)が未終了かつ、ホストレベル解析の結果により、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ホストレベル解析の入力としたパケットの情報を元にホスト内部解析を開始する(402、404)。その他の場合はホスト内部解析を開始しない(403)。ルータレベル解析終了時(410、411、412)、そのルータレベル解析と同時に開始されたホストレベル解析(たとえば、409で開始されたルータレベル解析に対する401で開始されたホストレベル解析)が未終了または、ルータレベル解析結果で得られたパケット生成ホストの発信元Etherアドレスを持つホストのアドレスとルータレベル解析の検索キーとしたパケットの発信元アドレスが異なる場合並びに、ホスト内部解析の対象となるホストが侵入経路解析装置の管理下に存在する場合に、ルータレベル解析結果ホストが送出したと断定されるパケットの情報を元にホスト内部解析を開始する(411、412)。その他の場合はホスト内部解析を開始しない(410)。このとき、同時に開始されたホストレベル解析によって既に別のホストに関するホスト内部解析プロセスが実行中であった場合(412)には、そのホスト内部解析プロセスを終了する(407)。ホスト内部解析終了時(405、406、408)、ホスト内部解析の入力としたパケットを生成したプロセスが、ネットワークを経由した外部装置からの命令を受信していた場合には、その命令を伝達したパケットを特定し、特定したパケットを入力とするホストレベル解析およびルータレベル解析を同時に起動する(405、406)。その他の場合はホストレベル解析、ルータレベル解析ともに開始しない(408)。これら全ての解析処理が終了した場合に侵入経路解析の終了とみなす(413)。

【0031】ここで、図4に示した例について概説する。ただし、便宜上、実行されるホストレベル解析、ルータレベル解析はいずれかのホストについてのホスト内部解析を可能であるという結果が得られるものとする。同様に、実行されるホスト内部解析結果は、407で終了される解析と408で終了する解析を除いて、ホスト内部解析の後に継続してホストレベル解析およびルータレベル解析を実行可能であるという結果が得られるものとする。ネットワークを流れるパケットを監視している侵入検知装置から侵入検知通知があり、401及び409においてホストレベル解析とルータレベル解析が同時に開始される。402においてホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元として、侵入経路解析装置と同じネットワークに属するホストのいずれかが検出される。なお、以下では、侵入経路解析装置と同じネットワークに属するホストを内部ホストと記す。また、401~402のホストレベル解析で検出された内部ホストを内部ホストAと称する。40

10

20

30

40

50

2においてホストレベル解析が終了したときに、終了したホストレベル解析と同時に開始されたルータレベル解析が未終了であるので、引き続きホスト内部解析が行われる。ホスト内部解析では、ホストレベル解析で検出された内部ホストAの内部プロセスについて解析が行われる。一方、410においてルータレベル解析が完了するが、ルータレベル解析での検出結果は、先に完了しているホストレベル解析の検出結果と同じなので、ホスト内部解析はそのまま実行される。405で、ホスト内部解析が完了し、内部ホストAが受信したパケットのうち侵入パケットの生成及び送信に参与したパケット（以下、侵入パケットと記す）が特定される。405でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。411において、ルータレベル解析が完了し、ルータレベル解析の結果、侵入パケットの送信元として内部ホストBが検出される。ルータレベル解析により内部ホストBが検出されたので、内部ホストBの内部プロセス状況についてホスト内部解析が開始される。一方、403で、ホストレベル解析が完了するが、既にルータレベル解析の結果によるホスト内部解析が実行されているため、ルータレベル解析の結果を優先し、411で実行されたホスト内部解析を継続する。406で、ホスト内部解析が完了し、内部ホストBが受信したパケットのうち侵入パケットの生成及び送信に参与した侵入パケットが特定される。406でホスト内部解析が完了したので、ホスト内部解析により特定された侵入パケットに対して、ホストレベル解析とルータレベル解析とが同時に開始される。404で、ホストレベル解析が完了し、ホストレベル解析の結果、侵入パケットの送信元候補として内部ホストCが検出される。そして、ホストレベル解析で検出された内部ホストCの内部プロセス状況についてホスト内部解析が開始される。一方、412で、ルータレベル解析が完了し、ホストレベル解析で検出された内部ホストCと異なる内部ホストDが侵入パケットの送信元として検出される。この場合、ルータレベル解析での検出結果はホストレベル解析での検出結果よりも正確性が高いので、内部ホストCに対して実行中であったホスト内部解析を終了し、ルータレベル解析で検出された内部ホストDの内部プロセスについてホスト内部解析を開始する（407）。図4の例では、ホスト内部解析の結果、内部ホストの侵入パケット生成・侵入に参与したパケットが検出されなかったため、内部ホストDを攻撃者の端末または攻撃者の端末が直結されたホストであると断定して全ての解析処理を終了する場合を示している（408、413）。

【0032】次に、ルータレベル解析の処理手順について説明する。まず、ルータレベル解析の基本的な原理について説明する。侵入経路解析装置は、侵入検知装置により、ホストへの侵入パケットが検知された場合に、検

知された侵入パケットのヘッダとデータ管理装置のデータベース内に格納されているヘッダ情報とを比較し、Etherアドレス及びTTLを除き侵入パケットのヘッダと同じ内容のヘッダ情報を抽出する。この抽出されたヘッダ情報は、EtherアドレスとTTL以外の情報が侵入パケットのヘッダと一致しているので、侵入パケットに関するヘッダ情報であると考えることができる。そして、抽出されたヘッダ情報について送信元Etherアドレス、宛先Etherアドレス、TTLの更新経過を順次遡ることにより侵入パケットの送信元を検出する。以上が、ルータレベル解析の基本的な原理である。では、次に、図5、図6並びに、図7を参照しながら、ルータレベル解析について具体的に説明する。

【0033】図5において、501から505はホスト、506から508はルータ、509から512は各機器を結ぶネットワーク、513から516はパケット収集装置、517は侵入検知装置、M1からM11は各機器が持つEtherアドレスを表している。

【0034】図6において、601から613はそれぞれ図5のホスト501から504の計4つのホストからホスト505（Etherアドレス：M11）へパケットのヘッダが全く等しい（Etherアドレス及びTTLを除く）攻撃パケットを送信したとき、図5の侵入検知装置517が検知するパケット608、609、612、613の何れかを検索キーとしてデータベース検索を行って得られた検索結果を表す。ただし、図6では、得られた検索結果をヘッダ情報のTTL値によって分類して記載してある。ヘッダ情報は便宜上、発信元Etherアドレス、宛先Etherアドレス、TTL値と、それら以外の情報（パケットの検索に用いた、ICMPプロトコルヘッダのType、Code、Checksum、IPプロトコルヘッダのIdentification、Protocol、発信元IPアドレス、宛先IPアドレス、TCP/UDPプロトコルヘッダの発信元ポート番号、宛先ポート番号、Checksum、TCPプロトコルヘッダのSequenceNumber、AcknowledgmentNumberなどが含まれ、図6ではXで表記）の4つに区別して表される。図7において、701は図6のパケット609を検索キーとしてルータレベル解析を行った侵入経路解析結果、702は図6のパケット612（またはパケット613）を検索キーとしてルータレベル解析を行った侵入経路解析結果を表している。

【0035】ここでは、図6のパケット609のルータレベル解析を行うものとする。パケット609を検索キーとしてデータベース検索を行った結果をIPプロトコルのTTL値によって分類すると図6のような分類が得られる。

【0036】次に、データベース検索により得られた結果に含まれるヘッダ情報のうち、パケット609のTT

L 値より小さい TTL 値を持つヘッダ情報を破棄する。これは、攻撃パケット送信ホストから攻撃を受けたホスト 505 までの経路上では、パケットの宛先 IP アドレスが受信したパケットの TTL 値が最小となることによる。したがって、TTL 値として 7 を持つパケット 612 とパケット 613 は、ここでデータベース検索結果から破棄される。

【0037】TTL 値がパケット 609 と同じ、8 のものがデータベース検索により得られた結果に存在する場合には、TTL 値が 8 に分類されるヘッダ情報から、パケット 609 と発信元 Ether アドレス並びに、宛先 Ether アドレスが等しいヘッダ情報以外のヘッダ情報を破棄する。したがって、パケット 610 とパケット 611 は、ここでデータベース検索結果から破棄される。

【0038】次に TTL 値が 9 のヘッダ情報について処理を行う。まず、TTL 値が 8 を持つパケットで残っているヘッダ情報（パケット 609）の発信元 Ether アドレスを持つルータ 508 が持つ全ての Ether アドレスを調べる。このとき、ルータ 508 は M10 と M9 を Ether アドレスとして持つことがわかる。次に、TTL 値が 9 に分類されるヘッダ情報のうち、M10 または M9 を宛先 Ether アドレスとして持つパケット 607 を選択し、残りを破棄する。したがって、パケット 605、パケット 606、パケット 608 は、ここでデータベース検索結果から破棄される。

【0039】同様に、TTL 値に 9 を持つパケットで残っているヘッダ情報（パケット 607）の発信元 Ether アドレス M8 を Ether アドレスとして持つルータ 507 が持つ全ての Ether アドレスを調べる。このとき、ルータ 507 は M8 と M7 を Ether アドレスとして持つことがわかる。次に、TTL 値が 10 に分類されるヘッダ情報のうち、M8 または M7 を宛先 Ether アドレスとして持つパケット 603 を選択し、残りを破棄する。したがって、パケット 601、パケット 602、パケット 604 は、ここでデータベース検索結果から破棄される。

【0040】TTL 値に 10 を持つパケットで残っているヘッダ情報（パケット 603）の発信元 Ether アドレス M3 を Ether アドレスとして持つルータが持つ全ての Ether アドレスを調べる。しかしながら、M3 はルータが持つ Ether アドレスではないため、M3 を Ether アドレスとして持つルータは検出されない。ここで、パケット 603 は、Ether アドレス M3 を持つホスト 503 から発信されたと断定する。したがって、パケット 609 は、ホスト 503 から発信されルータ 507 およびルータ 508 によって中継されホスト 505 へ到達したという、図 7 の 701 の結果が得られる。

【0041】図 6 のパケット 612（もしくはパケット

613）に関して上記の処理を行った場合は、図 5 のホスト 501 とホスト 502 がともにパケットの発信ホストとして特定され、図 7 の 702 のような結果が得られる。

【0042】以上のように、ルータレベル解析は、パケットの IP アドレスによらず解析を行うので、IP アドレスを詐称された場合でも正確に侵入パケットの送出ホストと中継経路を特定できる反面、一般的には解析に時間がかかる。

10 【0043】ここでは、図 8 を参照しながら侵入パケットの情報を初期入力とするホスト内部解析の説明を行う。図 8 において、810 はホスト（踏み台）、801 から 807 はホスト 810 上で起動されたプロセス、811、812 は外部装置、808 は外部装置 811 との通信並びに、809 は外部装置 812 との通信に使用されたホスト 810 上の通信ポートを表している。なお、外部装置とは、他のホストまたはルータを意味する。プロセス 801 からプロセス 807 の間には、他のプロセスによって起動された側と起動した側という、いわゆる  
20 プロセスの親子関係が成り立っている。たとえば、図 8 において、プロセス 805、プロセス 806 は、プロセス 804 によって起動されている。この場合、プロセス 805 およびプロセス 806 をプロセス 804 の子プロセス、プロセス 804 をプロセス 805、プロセス 806 親プロセスと呼ぶ。ここでは、ホスト 810 は外部装置 811 から外部装置 812 へ攻撃を行う際の踏み台ホストとして使用されたものとする。

【0044】侵入経路を外部装置 812 の側から前述のホストレベル解析もしくは、ルータレベル解析が既に行われており、解析の結果、パケットはホスト 810 の通信ポート 809 から送信されたことが特定されているものとする。このとき、そのパケット取得日時を検索キーとしてデータベースを検索し、その時間にホスト 810 の通信ポート 809 を使用していたプロセス（パケット生成プロセス）に関する情報（プロセス生成日時、プロセス終了日時、プロセス識別子、親プロセス識別子、実ユーザー識別子、実行ユーザー識別子、実グループ識別子、実行グループ識別子、実行ディレクトリ、実行コマンドパス、実行コマンドライン、通信開始日時、通信終了日時、通信先 IP アドレス、通信先 TCP/UDP ポート番号、通信 NIC に割り当てられていた Ether アドレスと IP アドレス、TCP/UDP ポート番号）を得る。このとき、パケット生成プロセスが外部装置からの接続による通信を確立していた場合（パケット受信プロセスが行われていた場合）は、通信開始日時、通信終了日時、通信先 IP アドレス、通信先 TCP/UDP ポート番号、通信 NIC に割り当てられていた Ether アドレスと IP アドレス、TCP/UDP ポート番号を検索キーとして、データベースを検索し、外部装置から受け取ったパケットを特定する。この特定したパケット  
50

は、ホスト 810 の攻撃パケットの生成に関与したパケットである。そして、この特定したパケットについて、ルータレベル解析及びホストレベル解析を行い、このパケットの送信元を特定する。パケット生成プロセスが外部装置からの接続による通信を確立していなかった場合は、同様の処理を親プロセスに対して行う。

【0045】パケット生成プロセスが外部装置からの接続による通信を確立していたプロセスが見つかるか、親プロセスが定義されないプロセス（オペレーティングシステムの特別なプロセス）にたどり着くまで、上記の処理を繰り返し行う。親プロセスが定義されないプロセスにたどりついた場合には、そのホストを、攻撃者が直接利用したコンピュータであると断定する。

【0046】図 8 の例では、プロセス 803 が外部装置からの接続による通信を確立していたプロセスとなるため、プロセス 803 に関する情報を検索キーとしてデータベースを検索し、プロセス 803 が外部装置から受け取ったパケットを特定する。

【0047】ホスト内部のプロセス情報を初期入力とするホスト内部解析（ホスト内部を監視する侵入検知装置により解析対象となるホストが特定された場合）では、上記のパケットの情報を初期入力とするホスト内部解析のホスト上でパケットを生成したプロセスに関する情報を得る処理から解析を開始し、後の処理は、パケットの情報を初期入力とする処理と同様である。

【0048】以上のように、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を並行して行うことから、解析結果の正確性を保証しつつ、高速に侵入経路解析を行うことができる。また、ヘッダ情報並びに、ホスト内部情報をデータ管理装置でデータベースにより集中管理するため、ホストレベル解析、ルータレベル解析並びに、ホスト内部解析を行う際に、侵入経路解析中は各装置間で通信を行いながら、経路上の各ルータを逐次追跡する必要がないことから侵入経路解析時間の短縮効果がある。

【0049】実施の形態 2。以上の実施の形態 1 では、過去における侵入に関しても追跡可能とするために、ネットワーク上を流れるパケットおよびホスト上のプロセスの情報を常時取得し、記録していた。この場合、記録したデータを保存するために、大容量の記憶領域を消費する。しかしながら、導入するシステムの環境によっては、データを保持しておくための大容量記憶領域の確保が難しい場合もあるため、以下のような方法により適宜情報を圧縮することもできる。第一に、記録する各パケットのデータのうち、侵入経路解析で用いる項目（パケット取得日時並びに、パケットを識別するために一般的に用いられるパケットヘッダ内の発信元 E t h e r アドレス、宛先 E t h e r アドレス、ICMP プロトコルヘッダの Type、Code、Checksum、IP プロトコルヘッダの I d e n t i f i c a t i o n、T T

L、Protocol、発信元 IP アドレス、宛先 IP アドレス、TCP/UDP プロトコルヘッダの発信元ポート番号、宛先ポート番号、Checksum、TCP プロトコルヘッダの Sequence Number、Acknowledgment Number）だけを記録していく。第二に、侵入経路解析装置より侵入経路データ提出要求があったときのみ各パケット取得装置並びに、各ホスト内部情報収集装置で同時に情報収集を開始する。どちらの場合も、解析するシステムの大きさにより、データを保持する期間を決めて一定期間を過ぎたデータから随時削除していくことも可能である。

【0050】以上のように、常時保持するデータの量を制限することで、侵入経路解析に使用される記憶領域容量を軽減できる。ただし、データを保持しておく期間は、適用するシステムの性能並びに、要求される解析結果の詳細度によって決定される。

【0051】実施の形態 3。以上の実施の形態 1 並びに実施の形態 2 では、少なくとも解析を行う段階においてデータベースに検索対象となるデータが格納されていれば侵入経路解析には影響を及ぼさない。したがって、各パケット取得装置並びに、各ホスト内部情報収集装置で収集したデータを常時データベース管理装置に格納する必要はなく、侵入経路解析を行わないときには、各パケット収集装置並びに、各ホスト内部情報収集装置で収集したデータを保持しておき、侵入経路解析を行う際に各装置から一斉に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することもできる。

【0052】以上の実施の形態 3 によれば、収集データの分散管理が可能であり、侵入経路解析未実行時のデータ管理装置上のリソースに対する負荷（記憶領域容量並びにデータ処理など）を削減できる。

【0053】実施の形態 4。以上の実施の形態 3 では、侵入経路解析を行う際に各装置から一斉に記録データ（パケットの情報並びに、ホスト上のプロセス情報）をデータ管理装置へ送信しデータベースへ格納することで、侵入経路解析未実行時の収集データの分散管理を行った。これに加え、各パケット収集装置上にルータレベル解析機能並びに、各ホスト内部情報収集装置上にホスト内部解析機能を備え、侵入経路解析装置が侵入経路解析のスケジューリング並びに、ホストレベル解析を行うようにした場合には、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。

【0054】以上の実施の形態 4 によれば、ネットワーク上に分散している各パケット収集装置並びに、各ホスト内部情報収集装置上へ侵入経路解析処理を分散しているため、侵入経路解析時に侵入経路解析装置にかかる計算負荷を軽減できる。加えて、実装上パケット収集装置並びに、ホスト内部情報収集装置がそれぞれルータ並びにホスト上に実装されていた場合、当該不正アクセス処

理が継続中である場合には、ルータやホストのその他の処理を意図的に遅延されることも可能であり、不正アクセス処理を遅延する効果もある。

【0055】実施の形態5. 以上の実施の形態1~4では、単一の侵入経路解析装置を用いた場合の実施の例であったため、侵入経路解析の範囲に限界がある。そこで、実施の形態5では、複数の侵入経路解析装置を用いて、より広範囲な侵入経路解析を行う方式について説明する。

【0056】図9において、901、902、903はそれぞれ異なる侵入経路解析装置、904、905、906はそれぞれ侵入経路解析装置901、902、903が経路解析可能なネットワーク、907~910は侵入経路上のホストを表している。なお、各ネットワークとも、図1に示したように、侵入検知装置、パケット収集装置等が配置されているものとする。各ホスト間を結ぶ直線上にはパケットを中継する複数のルータが存在している。図9では、ホスト907を攻撃者端末とし、攻撃者はホスト908およびホスト909を踏み台としてホスト910を攻撃したものとする。

【0057】侵入経路解析装置903は、前述の方法で侵入経路解析を行った結果、ホスト910への不正アクセスパケットは、侵入経路解析装置902によって追跡可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。このとき、侵入経路解析装置903は、ネットワーク905からネットワーク906へ送られてきたパケットの情報を含む検出依頼を侵入経路解析装置902に送信し、侵入経路解析の継続を依頼する。

【0058】検出依頼を受領した侵入経路解析装置902は、侵入経路解析装置903から送られてきたパケット情報を元に、実施の形態1~4に示す方式に従って侵入経路解析を行う。このとき、ネットワーク905上のホスト908およびホスト909が踏み台とされたこと、並びに、ホスト908は侵入経路解析装置901が解析可能なネットワーク上の装置（ホストまたはルータ）から送信されたパケットであると断定する。侵入経路解析結果を侵入経路解析装置903に送信する。

【0059】侵入経路解析装置903は、侵入経路解析装置902の解析結果に含まれる、侵入経路解析装置902からのパケット情報を含む検出依頼を侵入経路解析装置901へ送信し、侵入経路解析の継続を依頼する。

【0060】侵入経路解析装置901でも、侵入経路解析装置902と同様に侵入経路解析を行い、検出依頼のあったパケットは、ホスト907から発信されたことを特定し、解析結果を侵入経路解析装置903に送信する。

【0061】最終的に、侵入経路解析装置903は、ネットワーク906の解析結果、並びに、侵入経路解析装置902、侵入経路解析装置901から送信されてきた

結果から、ホスト907からホスト910までの一連の侵入経路を特定する。

【0062】以上の実施の形態5によれば、複数の侵入経路解析装置が連携し、個々のネットワーク内の解析結果を統合しているため、複数のネットワークにわたるような広範囲な侵入経路解析ができる。

【0063】以上の実施の形態1~5では、本発明に係る不正アクセス経路解析システム（侵入経路解析システム）について説明したが、実施の形態1~5に示した処理手順により本発明に係る不正アクセス経路解析方法も実現可能である。

【0064】ここで、実施の形態1~5に示した侵入経路解析システムの特徴を以下にて再言する。

【0065】実施の形態1~5に示す侵入経路解析システムは、以下の装置を有することを特徴とする。

1. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ネットワーク上を流れるパケットを収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するパケット収集装置（複数可能）。

2. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、オペレーティングシステムによって管理されるホスト上のプロセス管理情報並びに、そのプロセスのプロセス間通信履歴に関する情報（これらを総称してホスト内部情報と呼ぶことがある）を収集し、記録し、外部装置による記録データ送信要求発行時もしくは、定期的に外部装置へ記録データを送信するホスト内部情報収集装置（複数可能）。

3. ネットワーク上に存在するパケット収集装置並びに、ホスト内部情報収集装置へ記録データ送信要求発行後もしくは、定期的にパケット収集装置並びにホスト内部情報収集装置から送信される記録データを受信し、データベースに格納するデータ管理装置（複数可能）。

4. 外部装置からの命令を受信もしくは、自動もしくは、手動で起動し、ホストレベル解析機能、ルータレベル解析機能、ホスト内部解析機能を持ち、それぞれの解析を平行して実行可能である侵入経路解析装置（複数可能）。

5. ネットワーク上を流れるパケットを監視もしくはホストの内部状態を監視することで侵入を検知し、検知した情報を外部装置へ通知する侵入検知装置。

【0066】実施の形態1~5に示す侵入経路解析システムは、ヘッダ情報を検索キーとしてデータベース検索し、得られた複数の検索結果をパケット情報に含まれるTTL (Time to Live) データ、送信元Ethernetアドレス並びに、宛先Ethernetアドレスを用いて解析することを特徴とする。

【0067】実施の形態1~5に示す侵入経路解析システムは、ルータレベル解析と、ホスト内部情報を用いたホスト内部解析とを行うことを特徴とする。

【0068】実施の形態1～5に示す侵入経路解析システムは、ルータレベル解析並びに、パケット情報に含まれる発信元IPアドレスによるパケットの発信元解析を行うホストレベル解析並びに、ホスト内部解析を併用して侵入経路解析を高速化することの特徴とする。

#### 【0069】

【発明の効果】以上のように、本発明によれば、送信元検出処理及び内部プロセス解析処理を行うため、踏み台を介した不正アクセス、発信元アドレスを詐称した不正アクセスにも対応可能であり、解析結果の正確性を保証しつつ、高速に不正アクセス経路解析を行うことができる。

【0070】また、本発明によれば、第一の送信元検出処理と第二の送信元検出処理とを並行して行うため、第一の送信元検出処理により解析結果の正確性を保証することができ、また、第二の送信元検出処理により解析処理の高速化を図ることができる。

【0071】また、本発明によれば、パケットの収集及び内部プロセス情報の収集は、指示があった場合のみ行うため、ヘッダ情報及び内部プロセス情報の記憶のための記憶領域容量を軽減することができる。

【0072】また、本発明によれば、ヘッダ情報及び内部プロセス情報は、指示があった場合のみ送信することとしているため、不正アクセス経路解析を行わないときのシステムリソースに対する負荷を削減することができる。

【0073】また、本発明によれば、複数のネットワークに跨って不正アクセス経路解析を行うことができるた

め、広範囲に渡った不正アクセスの場合でも、正確かつ高速に不正アクセス経路解析を行うことができる。

#### 【図面の簡単な説明】

【図1】 侵入経路解析システムのシステム構成例を示す図。

【図2】 従来の技術を説明する図。

【図3】 従来の技術を説明する図。

【図4】 侵入経路解析スケジューリング例を示す図。

【図5】 ルータレベル解析例を説明するためのシステム構成図。

【図6】 ヘッダ情報の例を示す図。

【図7】 ルータレベル解析の結果の例を示す図。

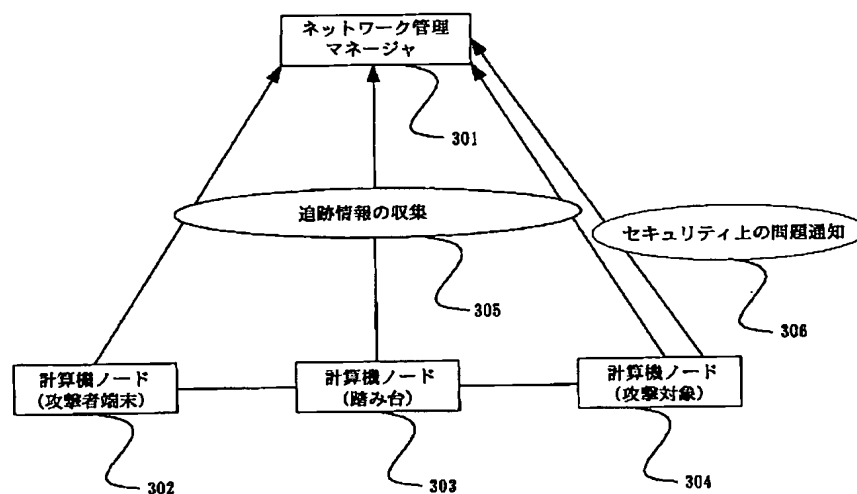
【図8】 ホスト内部解析例を説明するためのプロセス経過図。

【図9】 複数の侵入経路解析システムを用いた解析例を説明するためのシステム構成図。

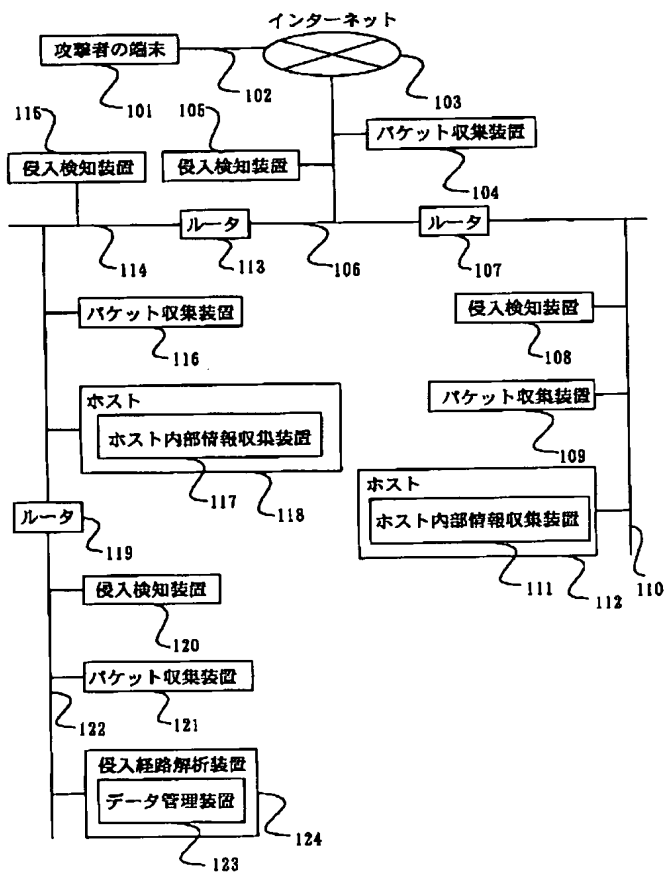
#### 【符号の説明】

101 攻撃者の端末、102 経路、103 インターネット、104 パケット収集装置、105 侵入検知装置、106 サブネットワーク、107 ルータ、108 侵入検知装置、109 パケット収集装置、110 サブネットワーク、111 ホスト内部情報収集装置、112 ホスト、113 ルータ、114 サブネットワーク、115 侵入検知装置、116 パケット収集装置、117 ホスト内部情報収集装置、118 ホスト、119 ルータ、120 侵入検知装置、121 パケット収集装置、122 サブネットワーク、123 データ管理装置、124 侵入経路解析装置。

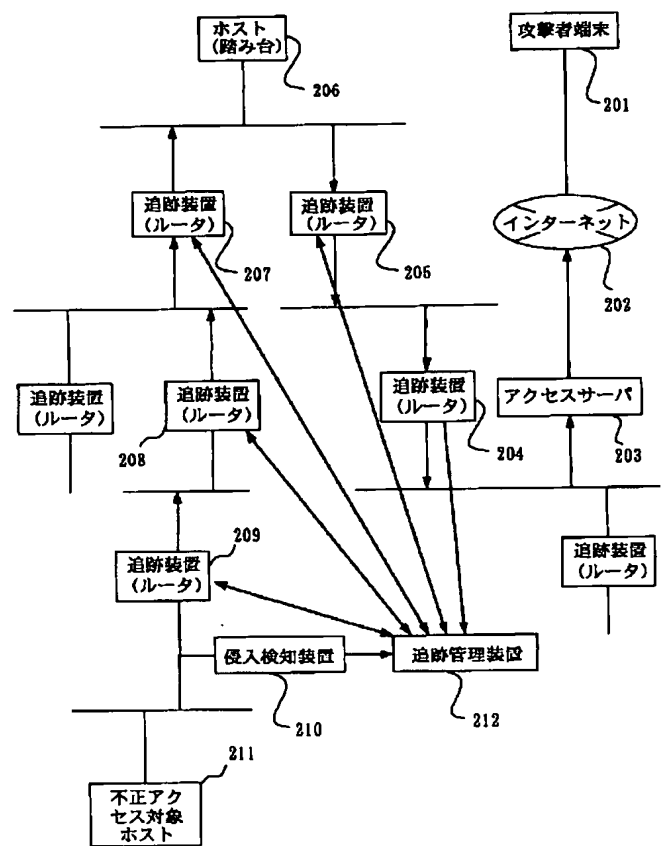
【図3】



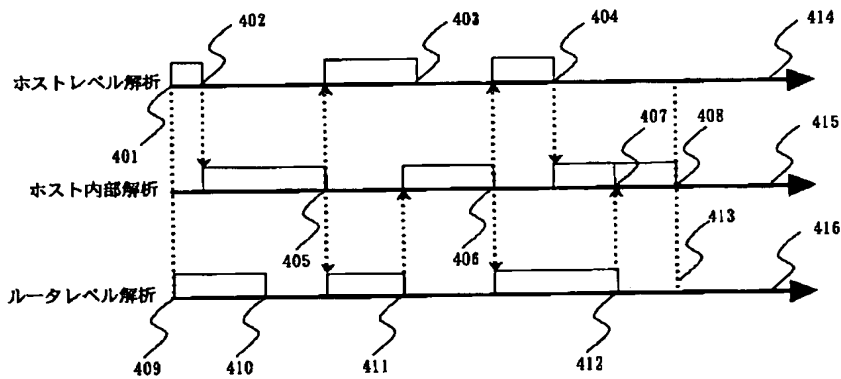
【図 1】



【図 2】

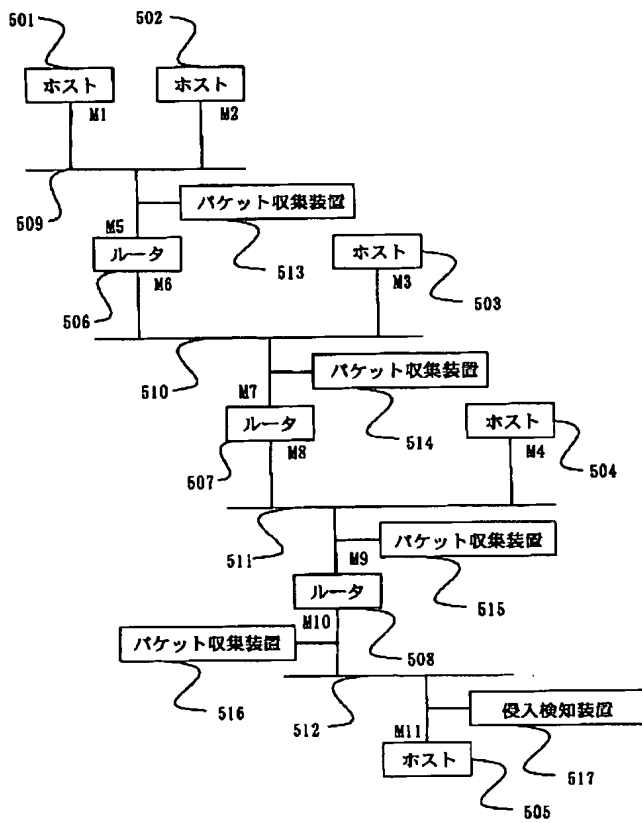


【図 4】

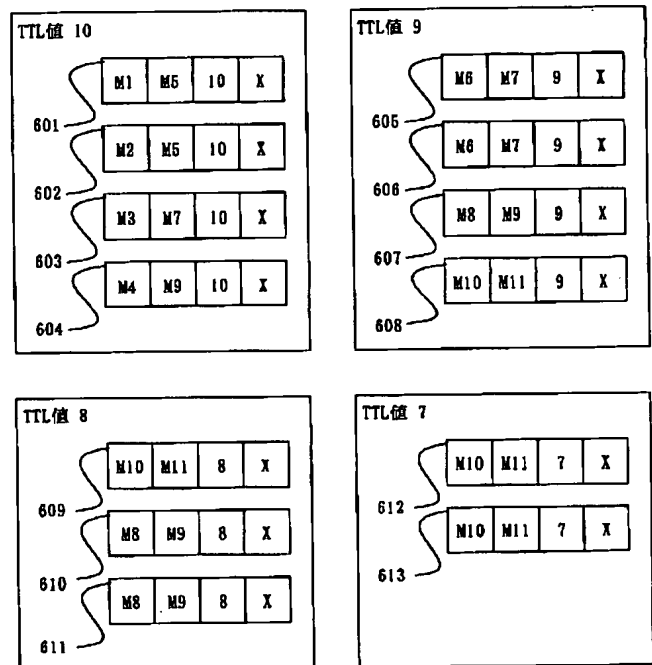




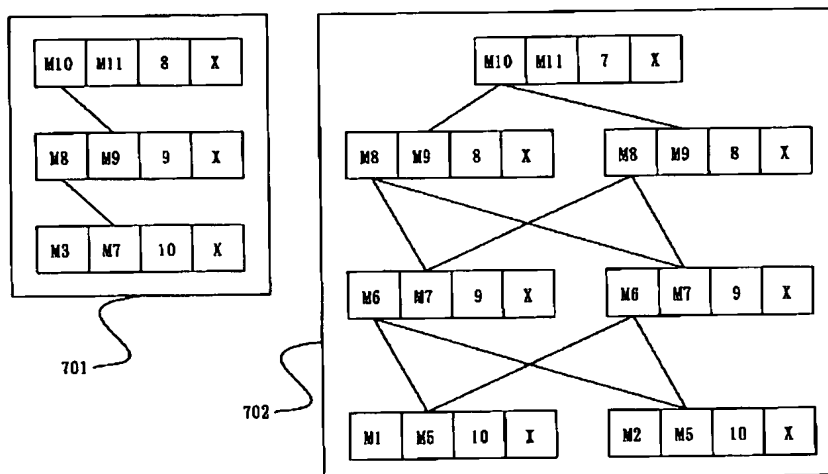
【図 5】



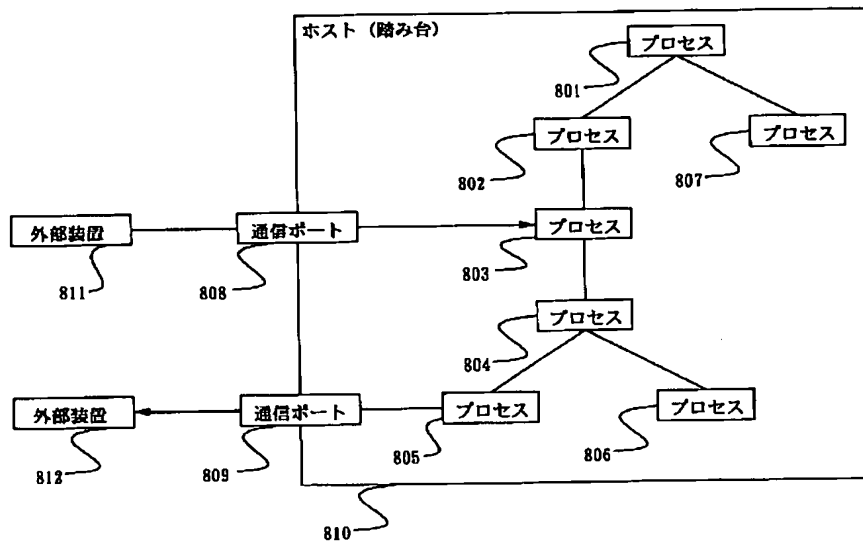
【図 6】



【図 7】



【図 8】



【図 9】

